

دانشگاه اصفهان

دانشکده مهندسی کامپیوتر

گزارش فاز اول پروژه تحلیل و طراحی سیستم­ها

سامانه ادله دیجیتال

گروه شماره ۱۶

گردآورندگان:

محمد محمدی

حیدرعلی الدیرانی

علی بهرامی

مهدی غفوری

سهیل کریمیان خوزانی

پارسا مظاهری

استاد راهنما: جناب دکتر محمدرضا شعرباف

دستیار آموزشی: خانم شیما مغزی

نیم‌سال دوم سال تحصیلی ۱۴۰۳ – ۱۴۰۴

فهرست مطالب

[فاز اول: مقدمات و شناسایی نیازها 3](#_Toc192939598)

[۱- مقدمه 3](#_Toc192939599)

[۱-۱- هدف 3](#_Toc192939600)

[۲-۱- قلمرو 3](#_Toc192939601)

[۳-۱- بیان مسئله 3](#_Toc192939602)

[۴-۱- تعاریف، واژگان و کوته‌نوشت‌ها 4](#_Toc192939603)

[۵-۱- مراجع 4](#_Toc192939604)

[۶-۱- طرح کلی 4](#_Toc192939605)

[۲- شرح کلی 5](#_Toc192939606)

[۱-۲- چشم­انداز محصول 5](#_Toc192939607)

[۱-۱-۲- واسط­های سیستم 5](#_Toc192939608)

[۲-۱-۲- واسط­های کاربری (UI) 6](#_Toc192939609)

[۳-۱-۲- واسط­های سخت­افزاری 6](#_Toc192939610)

[۴-۱-۲- واسط­های نرم­افزاری 6](#_Toc192939611)

[۵-۱-۲- واسط­های ارتباطی 6](#_Toc192939612)

[۶-۱-۲- واسط­های حافظه 7](#_Toc192939613)

[۷-۱-۲- واسط­های عملیاتی 7](#_Toc192939614)

[۸-۱-۲- نیازمندی­های سازگاری با محل نصب 7](#_Toc192939615)

[۲-۲- کارکرد محصول 8](#_Toc192939616)

[۳-۲- قوانین کسب‌وکار 8](#_Toc192939617)

[۴-۲- مشخصات کاربران 9](#_Toc192939618)

[۵-۲- قیود 9](#_Toc192939619)

[۶-۲- مفروضات و وابستگی­ها 10](#_Toc192939620)

# فاز اول: مقدمات و شناسایی نیازها

## ۱- مقدمه

در این فصل قصد داریم به تعیین و تبیین نیازمندی­های یک سامانه ادله دیجیتال بپردازیم. از دیرباز شاکیان برای اثبات حق از دست رفته­شان به یک مدرک و سند قابل­اعتماد و محکمه­پسند احتیاج داشتند و تا کنون هم این نیاز پابرجاست. امروزه با پیشرفت علم‌وفناوری[[1]](#footnote-2) نوع اسناد و مدارک نیز تغییر یافته­اند. به همین دلیل اهمیت استفاده از ادله دیجیتال در اثبات برخی ادعاها اهمیت بسیار زیادی به خود جلب کرده است.

### ۱-۱- هدف

در این سامانه[[2]](#footnote-3) قصد داریم برای افراد سکویی[[3]](#footnote-4) امن بنا کنیم تا ابتدا افراد احراز هویت[[4]](#footnote-5) شوند و سپس فرد شاکی مدارک و مستندات خود در زمینه جرائم اینترنتی[[5]](#footnote-6) به مقامات قضایی ارائه کند. سپس مدارک وی در کمال حفاظت و نگهداری صحیح در فرایندهای جمع­آوری و ذخیره­سازی، با ابزارهای به­روز هوش مصنوعی و به­دور از خطاهای انسانی یا بعضاً سوءنیت پالایش شده و در اختیار حکام قضایی قرار گیرد.

### ۲-۱- قلمرو

این سامانه به­منظور تسهیل فرایند بارگذاری، احراز صحت ادله، حفظ و نگهداری و در نهایت دادرسی در اماکن قضایی ایجاد شده است. این سامانه در دستگاه قضایی، نیروی انتظامی و پلیس فتا تعبیه می­شود و شاکیان و قضات در بستر اینترنت می­توانند فرایند دادخواهی یا رسیدگی به شکایات را رصد کنند. همچنین این در این سامانه قصد داریم تمامی مدارک و ادله دیجیتال من­جمله متن، تصویر و صدا را پشتیبانی کرده و در کمال حفاظت در اختیار مراجع ذی­صلاح قرار دهیم تا از برخی مسائل همچون جعل یا سرقت اسناد نیز جلوگیری لازم به عمل آید.

### ۳-۱- بیان مسئله

از دیرباز ارائه مدارک برای اثبات دعاوی حقوقی یک مسئله بسیار حیاتی بوده است که در بسیاری از موارد معرفی یک الی چند شاهد به دادگاه از چالش‌های اثبات حق یک فرد شاکی است. امروزه اما با پیشرفت تکنولوژی این فرایند با ارائه برخی مدارک همچون فیلم و عکس بسیار آسان­تر شده ­است. از سوی دیگر این پیشرفت باعث ایجاد روش­های نوین در زمینه جرائم اینترنتی مانند کلاهبرداری­های آنلاین یا جعل اسناد با کمک هوش مصنوعی[[6]](#footnote-7) شده است که پیچیدگی­های خاص خود را دارند و دیگر روش­های سنتی تحلیل شواهد به نسبت ناکارآمد شده است. از این‌سو این سامانه قصد دارد تا با کمک گرفتن از هوش مصنوعی روی به هوشمندسازی، تحلیل و بررسی و درنهایت تصمیم­گیری در خصوص ادله دیجیتال بیاورد.

### ۴-۱- تعاریف، واژگان و کوته‌نوشت‌ها

|  |  |  |
| --- | --- | --- |
| مخفف یا معادل فارسی | معادل انگلیسی | توضیح کلمه |
| فناوری | **Technology** | مجموع تکنیک‌ها و روش‌هایی است که در تولید کالاها یا تحقق اهداف معمولاً علمی استفاده می­شود |
| سامانه | **System** | مجموعه­ای متشکل از عناصر مرتبط با یکدیگر که مسئول انجام کار خاصی هستند؛ دستگاه. |
| سکو | **Platform** | محل ارائه خدمات و ارتباطات همگانی |
| جرائم سایبری | **Cybercrime** | جرائمی که در محیط مجازی رخ می­دهند |
| سرور | **Server** | مرکز ارسال پاسخ به درخواست‌های سیستم |
| هوش مصنوعی | **AI** | سیستم‌های کامپیوتری که با شبیه­سازی برخی کارهای انسان­ها را با منطق پیاده­سازی شده­اش انجام می­دهد |
| رابط کاربری | **UI** | بخشی که انسان می­توانند با کامپیوتر تعامل کند |
| **HTTPS** | **Hypertext markup language** | به معنای پروتکل انتقال ابرمتنی است و وظیفه­ی ارسال و دریافت داده­ها بین کاربر و سرور را بر عهده دارد |
| **HTML** | **Hypertext markup language** | زبان ساخت اسکلت اجزای یک سایت است |
| **CSS** | **Cascading style sheets** | زبان استایل دادن و ویرایش ظاهری اجزای سایت است |
| **JavaScript** |  | زبان برقراری ارتباط بین اجزای سایت و دستورات کاربر |
| **Captcha** |  | سوالی کوچک برای تمایز دادن بین انسان و کامپیوتر |
| **RAM** | **Random-Access Memory** | حافظه ای کوتاه مدت برای ذخیره موقت داده ها |
| **SSD** | **Sold State Drive** | حافظه ای برای ذخیره داده­ها که کار با آن سریع است |

جدول ۱

### ۵-۱- مراجع

Kung, David C. Object-oriented software engineering: an agile unified methodology. McGraw-Hill, 2014

### ۶-۱- طرح کلی

در این سند ابتدا اهداف و ویژگی­های این سیستم را بیان کرده و سپس به بیان شرح کلی، چشم­انداز محصول و بیان واسط­های مختلف سیستم از جمله واسط­های کاربر، واسط­های نرم­افزار و سخت­افزار و... می­پردازیم. سپس کارکردهای محصول، قیود، مفروضات و وابستگی­های سیستم مورد بررسی قرار می­گیرند و نهایتاً به نیازمندی­های محصول می­پردازیم تا یک تصویر جامع و کامل از سیستم ارائه شود.

## ۲- شرح کلی

در دنیای امروز، با پیشرفت فناوری و گسترش استفاده از اینترنت، نقش ادله دیجیتال در تحقیقات کیفری و روند دادرسی­های قضائی افزایش­یافته است. ازآنجاکه جرایم سایبری روزبه­روز پیچیده­تر و نوآورانه­تر می‌شوند، در این سیستم قصد داریم تا با کمک گرفتن از تکنولوژی‌های نوین مانند هوش مصنوعی و یادگیری ماشین در شناسایی و پیگیری مجرمان سایبری بپردازیم و از سیستم‌های سنتی که عمدتاً زمان­بر و کم­دقت هستند به یک سیستم بسیار سریع، آسان و با دقت بالا برسیم و دخالت‌های انسانی را تاحدامکان کاهش دهیم.

### ۱-۲- چشم­انداز محصول

سامانه مذکور با هدف فراهم‌آوردن سیستم‌های هوشمند برای تحلیل و شناسایی صحت ادله ارسالی توسط شاکی یا متهم به دنبال جلوگیری از جعل اسناد و مدارک، ایجاد شفاف­ترین ادله برای دستگاه­های قضایی و درنهایت فراهم‌کردن ایده­آل­ترین شرایط برای تصمیم­گیری مراجع قضایی با کمک هوش مصنوعی است. در این سامانه ما یک پاسخگوی هوش مصنوعی آنلاین برای رفع شبهه در خصوص برخی قوانین نیز تعبیه کرده‌ایم که افراد در هر ساعت از شبانه­روز می­توانند برای سؤالات خود پاسخی با دقت بالا دریافت کنند.

#### ۱-۱-۲- واسط­های سیستم

واسط­های سیستم به تبادل اطلاعات و ارتباط بین سیستم فعلی و سیستم­های خارجی کمک می­کنند و به چگونگی ارتباط با محیط خارج می­پردازد.

* دسترسی به پایگاه‌داده[[7]](#footnote-8) دولت من برای احراز هویت کاربران(قضات، شاکیان و متهمان) و ورود به سیستم
* دسترسی سامانه به سیستم دریافت سوءپیشینه افراد برای تصمیم­گیری بهتر
* دسترسی به یک سامانه ارسال پیامک دارای زمان انقضا برای دریافت کد احراز هویت ارسال شده به شماره تلفن به نام شخص حقیقی یا شرکت حقوقی
* دسترسی به یک سامانه تایید کد کپچا[[8]](#footnote-9) برای تعیین انسان بودن کاربر
* ارتباط با سیستم‌های ارتباطات صوتی و تصویری برای فراهم کردن امکانات تماس و ویدئو کنفرانس بین کاربران.
* دسترسی به سیستم‌های پردازش تصویر برای شناسایی و اعتبارسنجی اسناد هویتی مانند کارت ملی یا پاسپورت.
* ارتباط با سیستم‌های هشدار دهنده و امنیتی برای شناسایی تهدیدات سایبری

#### ۲-۱-۲- واسط­های کاربری[[9]](#footnote-10) (UI)

واسط کاربری نقطه تعامل و ارتباط بین انسان و کامپیوتر در یک دستگاه است. این واسط باید آن­قدر خوب باشد تا کاربر پس از اتصال به اینترنت و ورود به سامانه، بدون نیاز به آموزش جدی و تنها از طریق تجربه‌کردن بخش‌های مختلف دستگاه به‌خوبی به نیازهای خود جامه عمل بپوشاند. توجه کنید که بر اساس میزان سطح دسترسی به اطلاعات سامانه سطح رابط کاربری افراد با یکدیگر متفاوت است. یعنی برای مثال کارهایی که یک قاضی در سامانه می­تواند انجام دهد بسیار بیشتر از دسترسی‌های شاکی یا متهم است. این واسط‌ها باید ایمن، سریع، مقیاس‌پذیر و کاربرپسند باشند تا فرایند مدیریت، تحلیل و تبادل شواهد دیجیتال به‌راحتی و ساده‌ترین نحو انجام شود.

#### ۳-۱-۲- واسط­های سخت­افزاری

* هر شخص باید حداقل یک تلفن همراه یا کامپیوتر شخصی[[10]](#footnote-11) جهت اتصال به اینترنت و ورود به سایت داشته باشد.
* به یک بخش پایگاه­داده و سرور جهت ارسال و دریافت اطلاعات به کاربران احتیاج است.
* در اماکن قضایی به دستگاهی برای تمبر زدن و پلمب کردن نامه­های ارسالی نیاز داریم.
* جهت احراز هویت، هر کاربر(قضات، شاکیان و متهمان) نیازمند حداقل یک تلفن همراه یا رایانه شخصی دارای سیم‌کارت، به­منظور دریافت پیامک و استفاده از امکانات سامانه است.

#### ۴-۱-۲- واسط­های نرم­افزاری

برای استفاده از سامانه، کاربران ملزم به استفاده از مرورگرهایی نظیر Chrome، Mozilla Firefox و Microsoft Edge یا هر مرورگری که از ابزارهای توسعه سایت مثل HTML، CSS و JavaScript پشتیبانی می‌کند استفاده کنند. برای ذخیره، پردازش و... اطلاعات نیز به یک پایگاه­داده مانند MySQL، Oracle و... نیاز داریم.

#### ۵-۱-۲- واسط­های ارتباطی

این سامانه از پروتکل HTTPS[[11]](#footnote-12) برای برقراری ارتباط امن با سرور بهره­مند می­شود. برای ورود به سایت، از سامانه پیامکی که به شماره تماس که به نام خود شخص است ارسال می­شود. برخی اطلاع‌رسانی‌ها از طریق خود سیستم به کاربر نمایش داده می­شوند و برخی از اطلاع‌رسانی‌ها از طریق نامه رسمی به دست شخص مورد نظر می­رسند.

#### ۶-۱-۲- واسط­های حافظه

* استفاده از حافظه RAM[[12]](#footnote-13) جهت تسریع در فرایند پاسخگویی به کاربران
* استفاده از برنامه­نویسی بهینه و ساختمان داده‌های مناسب و سریع برای افزایش سرعت و کاهش مصرف حافظه
* استفاده از حافظه SSD[[13]](#footnote-14) برای پردازش، ذخیره و بازیابی اطلاعات در سریع‌ترین زمان ممکن

#### ۷-۱-۲- واسط­های عملیاتی

* این سامانه نیاز به یک پایگاه‌داده قدرتمند دارد که بتواند داده­های مختلف مانند فیلم، عکس، صدا و متن را به صورت لحظه­ای ذخیره و به‌روزرسانی کند. این پایگاه‌داده باید قابلیت مدیریت حجم بالای داده­ها را داشته باشد.
* این سامانه نیاز به ابزارهایی دارد که داده­های پاک شده را برای ما بازیابی کند (مثل پیام­های پاک شده یا تاریخچه مرورگر پاک شده).
* این سامانه نیاز به ابزارهایی برای تشخیص داده‌های جعلی دارد. برخی از این ابزارها عبارت‌اند از:
* **:PhotoDNA** برای تشخیص تصاویر جعلی یا غیرمجاز.
* **:Triage-G2 ‌‌** ابزار پیشرفته برای تحلیل و تشخیص جعل در داده‌های دیجیتال.
* این سامانه نیازمند یک سیستم پیامکی برای اطلاع‌رسانی به شهروندان به‌خصوص شاکیان و متهمان جهت اطلاع‌رسانی است.
* این سامانه نیاز به یک سیستم احراز هویت خودکار دارد تا بتواند کاربران را به‌صورت ایمن شناسایی و تأیید کند. این سیستم می‌تواند از روش‌هایی مانند احراز هویت دومرحله‌ای[[14]](#footnote-15) استفاده کند.

#### ۸-۱-۲- نیازمندی­های سازگاری با محل نصب

ازآنجایی‌که سیستم ما بر روی یک سایت پیاده­سازی خواهد شد، افراد برای دسترسی و استفاده از سایت لازم دارند ابزارهایی همچون تلفن همراه، رایانه و در کل هر وسیله‌ای که بتوان یک مرورگر را روی آن نصب کرد در اختیار داشته باشند تا پس از اتصال به اینترنت وارد سایت شوند و از امکانات تعبیه شده استفاده لازم را به عمل بیاورند.

### ۲-۲- کارکرد محصول

* این سامانه با شناسایی کلاهبرداران باعث ایجاد فضایی امن برای کاربران فضای مجازی می‌شود.
* این سامانه با استفاده از ابزارهای مختلف در تشخیص مدارک جعلی به کاربران کمک می‌کند که اخبار دروغین را تشخیص بدهند.
* این سامانه با استفاده از هوش مصنوعی گنجانده شده در خود می­تواند بدون نیاز به ورود به سیستم قضایی به سؤالات و ابهامات قانونی شما در سریع­ترین زمان ممکن بهترین پاسخ را ارائه دهد.
* این سیستم‌ها می‌توانند با قراردادن اطلاعات در اختیار پلیس کار نیروهای پلیس را تسهیل ببخشد.
* این سیستم‌ها می‌توانند با شناسایی حملات ddos از آسیب به سرورها جلوگیری کنند.
* این سامانه با ویژگی غیرحضوری بودن خود می­تواند حتی‌الامکان از ایجاد ترافیک جلوگیری کرده و ردپای کربن[[15]](#footnote-16) را نیز به طرز چشمگیری کاهش دهد.
* این سامانه قابلیت مشاهده و رصد لحظه‌ای پرونده را نیز فراهم می­کند.

### ۳-۲- قوانین کسب‌وکار

قوانین کسب­وکار شامل مجموعه­ای از مقررات و قوانین حقوقی است که باید رعایت شوند. در ادامه به برخی از این قوانین به­کارگرفته­شده در این سامانه پرداخته می‌شود.

* هر شخص برای ورود به سامانه باید شماره همراهی به نام خود داشته باشد که پیامک تأیید کاربر برای آن شماره ارسال شود.
* مقامات قضایی باید مجوز و مدرک لازم را برای قضاوت و اجرای احکام داشته باشند و آن را بارگذاری کنند.
* برای پذیرش ادلة دیجیتال در محاکم، لازم است که صحت و تمامیت آنها حفظ شود. این امر معمولاً از طریق استفاده از تکنیک‌های درهم­سازی[[16]](#footnote-17) و ارائة شواهدی مبنی بر عدم تغییر یا دست‌کاری داده­ها انجام می­شود.
* جهت حفظ امنیت اطلاعات کاربر، اگر کاربر به مدت ۱۵ دقیقه از سامانه استفاده نکند و خارج نشود، سامانه به طور خودکار باید کاربر را از دسترس خود خارج کند.
* در صورت سه بار بی­توجهی به نامه ارسالی از سمت دادگاه، قاضی می­تواند حکم جلب شخص را صادر کند.
* اطلاعات کاربران را به‌دقت محافظت کرده و از هرگونه سوءاستفاده یا نقض حریم خصوصی آنها جلوگیری شود.
* به شواهد دیجیتالی که توسط پلیس ضبط شده است به‌عنوان شواهد شخص اول و شواهد دیجیتالی که از منابع دیگر گرفته شده است به‌عنوان شواهد شخص ثالث اشاره خواهیم.
* سیستم باید برای ذخیره و جلوگیری از ازدست‌رفتن داده­های کاربران به طور منظم از پایگاه­داده.
* اطمینان از انطباق سیستم با استانداردها و مقررات ملی و بین­المللی مرتبط با مدیریت ادله دیجیتال.
* تنظیم سطوح دسترسی برای کاربران مختلف بر اساس نقش‌ها و مسئولیت­هایشان، به­منظور جلوگیری از دسترسی غیرمجاز به داده­ها.

### ۴-۲- مشخصات کاربران

سامانه ادله دیجیتال توسط گروه‌های مختلفی از کاربران مورد استفاده قرار می‌گیرد که هر یک نقش‌ها و مسئولیت‌های خاصی در فرایند مدیریت، تحلیل و استفاده از این ادله دارند. در ادامه، انواع کاربران این سامانه‌ها و توضیح مختصری درباره هر یک ارائه شده است:

* کاربران عمومی: در برخی موارد، افراد عادی ممکن است نیاز به استفاده از سامانه‌های مدیریت ادله دیجیتال داشته باشند، مثلاً برای ارائه شواهد در پرونده‌های مدنی یا پیگیری مسائل حقوقی شخصی.
* وکلای مدافع: وکلای مدافع از این سامانه‌ها برای بررسی شواهد دیجیتال مرتبط با موکلان خود استفاده می‌کنند. آنها می‌توانند با تحلیل این شواهد، دفاعیات مؤثرتری ارائه دهند و از حقوق موکلان خود دفاع کنند.
* قضات و دادستان‌ها: این گروه از کاربران برای بررسی و ارزیابی شواهد دیجیتال در فرایندهای قضایی از سامانه‌های مدیریت ادله دیجیتال بهره می‌برند. دسترسی به شواهد معتبر و مستند به آنها کمک می‌کند تا تصمیمات قانونی دقیق‌تری اتخاذ کنند.
* کارشناسان جرم‌شناسی دیجیتال: این افراد مسئول جمع‌آوری، تحلیل و تفسیر داده‌های دیجیتال به‌منظور کشف شواهد مرتبط با جرایم سایبری هستند. آنها با استفاده از ابزارها و تکنیک‌های تخصصی، شواهد را استخراج و برای ارائه در محاکم قضایی آماده می‌کنند.
* مأموران اجرای قانون: پلیس و سایر مأموران اجرای قانون از سامانه‌های مدیریت ادله دیجیتال برای دسترسی سریع و مؤثر به شواهد الکترونیکی استفاده می‌کنند. این سامانه‌ها به آنها امکان می‌دهد تا در تحقیقات خود به داده‌های مورد نیاز دسترسی داشته باشند و روند پیگیری پرونده‌ها را تسریع کنند.
* مدیران سیستم و فناوری اطلاعات: این افراد مسئول نگهداری، به‌روزرسانی و امنیت سامانه‌های مدیریت ادله دیجیتال هستند. آنها اطمینان حاصل می‌کنند که سامانه‌ها به‌درستی کار می‌کنند و داده‌ها در برابر تهدیدات محافظت می‌شوند.

### ۵-۲- قیود

در این بخش به محدودیت‌های پیشرو می‌پردازیم:

* حجم بالای داده‌ها: سیستم باید توانایی مدیریت و پردازش حجم زیادی از داده‌های دیجیتال را از جمله عکس، ویدئو و صدا را داشته باشد.
* محدودیت در ثبت­نام: هر کاربر(قضات، شاکیان و متهمان) فقط با یک کد ملی و یک شماره تماس می­تواند ثبت­نام کند.
* دقت و قدرت تحلیل داده‌ها: دادهایی که از طریق هوش مصنوعی تحلیل می‌شوند باید دقت بالایی داشته باشد و بتواند نوع جرایم را تشخیص دهد.
* امنیت: سیستم باید از رمزنگاری‌های قوی همچون RSA و AES-256 استفاده کند تا بتواند از نفوذ و دست‌کاری جلوگیری کند.
* حفظ حریم خصوصی: باید اطلاعات خصوصی کاربر در سیستم مطابق استانداردهای بین‌المللی و تابع حفاظت از داده‌ها و حریم خصوصی ایران حفظ شود.
* محدودیت در سخت‌افزار و پردازش: برای پردازش داده‌های حجیم ما نیازمند زیرساخت قوی هستیم که می‌توان به سرور و پردازنده‌های سریع اشاره کرد.
* توانایی ارتباط با سایر سامانه‌ها: سیستم باید قابلیت اتصال به پایگاه‌داده‌های پلیس و نهادهای قضایی را داشته باشد.
* اعتبار سیستم: سیستم باید شواهد و مدارک دیجیتالی را به‌گونه‌ای غیرقابل‌تغییر و ویرایش کند که نهادهای پلیس و قوه قضاییه به این سیستم اعتماد داشته باشند.
* محدودیت زمانی در پردازش: برخی از پرونده‌ها نیازمند پردازش سریع اطلاعات هستند پس باید مدت‌زمان پردازش تاحدامکان کم باشد.
* میزان دسترسی کاربران به سیستم: بتوان سیستمی طراحی کرد که به‌صورت لایه‌ای باشد و دسترسی کاربران محدود باشد.
* پشتیبانی از کاربران به‌صورت هم‌زمان: سیستم باید بتواند بدون کاهش کارایی، هجمه‌ای را از کاربرانی که به‌صورت هم‌زمان از آن سیستم استفاده می‌کنند به­خوبی مدیریت کند.

### ۶-۲- مفروضات و وابستگی­ها

مفروضات:

* کاربر باید کد ملی و یک شماره همراه به نام خودش داشته باشد.
* کاربر باید از حداقل سواد خواندن و نوشتن برخوردار باشد.
* کاربر باید از روش­های کار با وسایل هوشمند مثل کامپیوتر یا گوشی دارای حداقل‌های یادگیری باشد.

وابستگی‌ها:

* برای کار با سامانه به یک بستر اینترنت پرسرعت نیازمندیم.
* به یک سامانه ارسال پیام کوتاه برای احراز هویت کاربران احتیاج است.
* سامانه به یک سیستم پرداخت آنلاین نیاز دارد.
* برای ثبت، حفاظت و بازیابی اطلاعات کاربران به یک پایگاه­داده کلان نیازمندیم.

## ۳- نیازمندی­ها

### ۱-۳- تبیین نیازمندی­های کارکردی

#### ۱-۱-۳- ثبت­نام کاربران (مراجع قضایی، شاکیان و متهمان)

1. باید یک بخش دادرسی توسط هوش مصنوعی ایجاد شود که شخص بدون ورود به سامانه سؤالات و ابهامات خود را از آن بپرسد و درگیر فرایند شکایت نشود. همچنین بهترین و دقیق­ترین پاسخ خود را دریافت کند.
2. ثبت‌نام با شماره تماس منطبق با کد ملی و ایجاد رمز باید انجام شود.
3. ثبت‌نام با شماره تماس منطبق با اسم شخص باید امکان‌پذیر باشد.
4. رعایت قالب نوشتاری در واردکردن شماره و کد ملی الزامی است.
5. سامانه باید قابلیت تشخیص ربات بودن یا نبودن شخص را با کپچا داشته باشد.
6. ثبت‌نام با ایمیل باید در سامانه امکان‌پذیر باشد.
7. سامانه ارسال پیامک تأیید به ایمیل[[17]](#footnote-18) شخص باید تعبیه شود.
8. سامانه باید قابلیت تشخیص یکتا بودن اطلاعاتی مانند شماره تماس و کد ملی را داشته باشد.
9. در صورت هر گونه تکراری بودن شماره همراه به کاربر اخطار دهد.
10. در صورت هر گونه تکراری بودن کد ملی به کاربر اخطار دهد.
11. سامانه باید پس از ۳ بار اشتباه‌کردن کاربر در واردکردن رمز یا کد ملی دسترسی او را به مدت ۱۵ دقیقه محدود کند.
12. ثبت اطلاعات در پایگاه­داده باید انجام شود.
13. تأیید کاربر با کد امنیتی از طریق پیامک باید امکان‌پذیر باشد.
14. فیلم آموزشی نحوه ثبت‌نام باید برای کاربران فراهم شود و لینک آن در صفحه لاگین[[18]](#footnote-19) قرار داده شود.
15. گزینه فراموشی رمز عبور و گزینه بازیابی حساب کاربری باید قرار داده شود.

#### ۲-۱-۳- مرحله پس از ورود

##### ۱-۲-۱-۳- دستگاه‌های قضایی (قضات، وکلا، نیروی انتظامی و...)

1. امکان دریافت ادله بر اساس میزان دسترسی افراد به اسناد اعمال شود.
2. امکان مشاهده نظر هوش مصنوعی در خصوص ادله ارائه شده فراهم شود.
3. امکان درخواست گرفتن ادله بیشتر از شاکی یا متهم قرار داده شود.
4. امکان ارسال به نهادهای دیگر مانند دادگاه، دادسرا، شهرداری و... در صورت نیاز فراهم شود.
5. امکان صدور حکم جلب در صورت مراجعه‌نکردن شاکی یا متهم به دادگاه پس از ۳ نامه در دسترس قرار گیرد.
6. ثبت نظر نهایی در خصوص شکایت و نشان‌دادن نتیجه به شاکی یا متهم ایجاد شود.
7. ارسال نتیجه نهایی به دست شاکی یا متهم در کنار ثبت در سامانه فراهم شود.
8. ثبت و ذخیره جزئیات کامل پرونده در پایگاه­داده برای مشاهده متهم و شاکی ایجاد شود.
9. امکان جستجو با شماره پرونده در بین اسناد مجاز (قابل‌دسترسی توسط مرجع قضایی) پایگاه­داده فراهم شود.
10. امکان معرفی به پلیس در صورت جعلی بودن ادله دیجیتال از جمله صدا، تصویر، متن و در کل هر نوع مدرک تعبیه شود.
11. امکان نظر دادن در خصوص رفتار سامانه و دیدن نظرات بقیه به‌صورت پیام متنی در اختیار کاربر قرار گیرد.
12. امکان ثبت نوبت دادگاه برای مراجع قضایی و اطلاع­رسانی به شاکی و متهم فراهم شود.
13. مرجع قضایی بتواند به سامانه دریافت سوءپیشینه دسترسی داشته باشد تا بهتر بتواند تصمیم بگیرد.
14. مرجع قضایی باید به سامانه وضعیت سلامت جسم و روان شاکی یا متهم دسترسی داشته باشد.
15. کتاب قوانین جمهوری اسلامی ایران در قالب یک فایل قابل‌جستجو در دسترس مرجع قضایی باشد.
16. پلیس باید به سامانه معاینه فنی، تعویض پلاک و... فرد متهم دسترسی داشته باشد.
17. امکان جریمه‌کردن آنلاین فرد خاطی توسط پلیس باید فراهم شود.

##### ۲-۲-۱-۳-شاکی و متهم

1. ثبت و ویرایش ادله دیجیتال برای شاکی یا متهم باید فراهم شود.
2. ثبت تاریخ و ساعت ادله ارائه شده برای دسترسی بهتر مراجع قضایی تعبیه شود.
3. طبقه‌بندی ادله توسط هوش مصنوعی پس از بارگذاری توسط متهم یا شاکی انجام شود.
4. تشخیص جعلی بودن یا نبودن صوت و تصویر و متن توسط هوش مصنوعی انجام شده و برای نتیجه نهایی به دست مرجع قضایی برسد.
5. امکان بررسی فرایند قضایی و مشاهده پرونده در جریان فراهم شود.
6. امکان نظر دادن در خصوص رفتار سامانه و دیدن نظرات بقیه به‌صورت پیام متنی در اختیار افراد قرار گیرد.
7. درگاه پرداخت آنلاین برای بررسی شکایات شاکیان تعبیه شود تا از پرداخت حضوری یا رشوه جلوگیری شود.
8. شاکی باید بتواند هر زمان که خواست از شکایت خود صرف‌نظر کرده و پرونده به بایگانی رود.
9. متهم باید بتواند هر زمان که خواست اظهارات شاکی را تأیید کند و پرونده مختومه گردد.
10. شاکی و متهم باید بتوانند هر زمان که خواستند از دادگاه درخواست وکیل کنند.
11. مدارک هویتی مثل آدرس منزل، شماره تماس، کد ملی و... شاکی و متهم باید از دسترس یکدیگر خارج شود و تنها با اجازه مرجع قضایی این مدارک در اختیار متهم یا شاکی قرار گیرند.

### ۲-۳- تبیین نیازمند­های غیرکارکردی

#### ۱-۲-۳- امنیت

* داده‌های ذخیره‌شده باید با الگوریتم‌های رمزنگاری قوی (AES-256, RSA) محافظت شوند.
* سیستم باید دارای احراز هویت چندمرحله‌ای[[19]](#footnote-20) برای کاربران حساس باشد.
* امکان شناسایی و جلوگیری از حملات سایبری مانند DDoS، SQL Injection و XSS وجود داشته باشد.
* سیستم باید قابلیت ردیابی تغییرات را داشته باشد.
* در صورت تشخیص فعالیت مشکوک، سیستم باید هشدارهای امنیتی فوری صادر کند و به طور خودکار قفل شود.
* قابلیت کنترل سطح دسترسی کاربران بر اساس نقش و مسئولیت آن‌ها فراهم شود.

#### ۲-۲-۳- کارایی و عملکرد

* تأخیر پاسخگویی سیستم به درخواست‌های کاربران نباید بیش از حد طولانی باشد.
* سیستم باید حداقل ۱۰۰۰ پرونده را به طور هم‌زمان بدون افت کارایی پردازش کند.
* سیستم باید توانایی پردازش حداقل ۱۰ ترابایت داده در ماه را داشته باشد.
* سامانه باید از رایانش توزیع‌شده برای پردازش سریع‌تر داده‌ها استفاده کند.
* پردازش و تحلیل داده‌های چندرسانه‌ای (تصویر، ویدئو، صوت) باید در کمترین زمان ممکن انجام شود.
* قابلیت پردازش سریع حجم بالای داده‌های لاگ[[20]](#footnote-21) سیستم‌های شبکه و امنیتی.
* بهینه‌سازی مصرف منابع سخت‌افزاری برای افزایش بهره‌وری سیستم.

#### ۳-۲-۳- قابلیت اطمینان و دسترس‌پذیری

* سیستم باید ۲۴/۷ [[21]](#footnote-22)(بدون توقف) فعال باشد.
* در صورت خرابی، سیستم باید حداکثر ظرف ۳۰ دقیقه بازیابی شود.
* سیستم باید از چندین سرور پشتیبان خودکار برای جلوگیری از ازدست‌رفتن اطلاعات استفاده کند.
* اگر یک سرور از کار بیفتد، سیستم باید بدون تأخیر به سرور جایگزین منتقل شود.
* قابلیت بازگردانی سریع اطلاعات حذف‌شده یا خراب‌شده وجود داشته باشد.
* سرویس‌ها باید به‌گونه‌ای طراحی شوند که در صورت افزایش کاربران، بدون افت عملکرد مقیاس‌پذیر باشند.

#### ۴-۲-۳- مقیاس‌پذیری و توسعه‌پذیری

* طراحی نرم‌افزار باید به‌گونه‌ای باشد که افزودن قابلیت‌های جدید بدون نیاز به تغییرات اساسی امکان‌پذیر باشد و بدون نیاز به توقف سرویس انجام شود.
* سیستم باید با سرویس‌های ابری[[22]](#footnote-23) سازگار باشد.
* سامانه باید امکان اتصال به [[23]](#footnote-24)APIهای سایر سیستم‌های قانونی و امنیتی را داشته باشد.
* هزینه نگهداری سیستم باید بهینه و مقرون‌به‌صرفه باشد.

1. Technology [↑](#footnote-ref-2)
2. System [↑](#footnote-ref-3)
3. Platform [↑](#footnote-ref-4)
4. Authentication [↑](#footnote-ref-5)
5. Cybercrime [↑](#footnote-ref-6)
6. AI (Artifical Intelligence) [↑](#footnote-ref-7)
7. Database [↑](#footnote-ref-8)
8. Captcha [↑](#footnote-ref-9)
9. User Interface [↑](#footnote-ref-10)
10. PC (Personal Computer) [↑](#footnote-ref-11)
11. HyperText Transfer Protocol Secure [↑](#footnote-ref-12)
12. Random Access Memory [↑](#footnote-ref-13)
13. Sold State Drive [↑](#footnote-ref-14)
14. Two-Step Verification [↑](#footnote-ref-15)
15. Carbon Footprint [↑](#footnote-ref-16)
16. hashing [↑](#footnote-ref-17)
17. Email [↑](#footnote-ref-18)
18. Login [↑](#footnote-ref-19)
19. MFA [↑](#footnote-ref-20)
20. Log [↑](#footnote-ref-21)
21. 24 hours a day of 7 days a week [↑](#footnote-ref-22)
22. Cloud-based solutions [↑](#footnote-ref-23)
23. Application Programming Interface [↑](#footnote-ref-24)